UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,193	12/03/2003	Bernard E. Brady JR.	M0929.70003US00	4674

46630 7590 04/16/2009
EMC Corporation
c/o WOLF, GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
MACILWINEN, JOHN MOORE JAIN	
ART UNIT	PAPER NUMBER
2442	

MAIL DATE	DELIVERY MODE
04/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,193	BRADY ET AL.	
	Examiner	Art Unit	
	John M. Macllwinen	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-17,20-30,33-39,82-85,88-94 and 109-128* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 7-17, 20-30, 33-39, 82-85, 88-94, 109-128* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 12/18/2008 have been fully considered.

2. In light of their claim amendments, Applicant arguments regarding the previous rejections made under 35 USC 101 are persuasive and thus said rejection has been withdrawn.

3. Applicant continues by arguing the rejections made under 35 USC 102 in view of Khanolkar. The Examiner agrees that Khanolkar does not teach Applicant's claim language as amended, and thus said rejections have been withdrawn. However, after further consideration, a new grounds of rejection has been made under 35 USC 103; said grounds is discussed further below.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 10 – 13, 14, 23 – 26, 27, 36-39, 82, 91-94 and 109 - 128 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar (US 7,127,743 B1) in view of Wiley (US 7,017,185 B1).

6. Regarding claims 1, Khanolkar shows in a computer system comprising a plurality of nodes interconnected for communication via a network, a method including

acts of capturing in a data structure a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event (Khanolkar, col. 2 lines 10 - 67, col. 3 lines 57 - 65 and col. 4 lines 15 - 30)

identifying a data element within the notification (Khanolkar, col. 6 lines 2 - 8, col. 7 lines 1- 3)

wherein the data element identifies a notification type for the notification, an originating IP address for the notification and/or a destination IP address for the notification (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55) and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55).

Khanolkar does not explicitly show all of where the data structure is a first data structure of a plurality of data structures, the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic;

updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded.

Wiley shows where the data structure is a first data structure of a plurality of data structures (Wiley, col. 4 lines 40 – 65), the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic (Wiley, col. 6 lines 11 – 35, col. 7 lines 1 – 51);

updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded (Wiley, col. 5 lines 25 – 67, col. 7 lines 1 – 51).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Khanolkar with that of Wiley in order to provide faster access to stored data (Wiley, col. 2 lines 17 – 28).

7. Regarding claim 14, Khanolkar in view of Wiley further show at least one computer-readable medium encoded with instructions which, when executed by a computer, perform a method in a computer system comprising a plurality of nodes interconnected for communication via a network, a method including acts of:

(A) capturing, in a first data structure of a plurality of data structures (Wiley, col. 4 lines 40 – 65), a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event (Khanolkar, col. 2 lines 10 – 67, col. 3 lines 57—65, col. 4 lines 15 – 30), the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic (Wiley, col. 6 lines 11 - 35, col. 7 lines 1 – 51);

(B) identifying a data element within the notification (Khanolkar, col. 6 lines 2 – 8, col. 7 lines 1 - 3);

(C) updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded (Wiley, col. 5 lines 25 – 67, col. 7 lines 1 – 51);

wherein the data element identifies a notification type for the notification, an originating IP address for the notification and/or a destination IP address for the notification (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55) and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55).

8. Regarding claim 27, Khanolkar in view of Wiley further show a system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising at least one processor programmed to implement:

a capture controller, said capture controller capturing, in a first data structure of a plurality of data structures (Wiley, col. 4 lines 40 – 65), a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event (Khanolkar, col. 2 lines 10 – 67, col. 3 lines 57—65, col. 4 lines 15 – 30), the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic (Wiley, col. 6 lines 11 - 35, col. 7 lines 1 – 51);

an identification controller, said identification controller identifying a data element within the notification (Khanolkar, col. 6 lines 2 – 8, col. 7 lines 1 - 3);

an update controller, said update controller updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded (Wiley, col. 5 lines 25 – 67, col. 7 lines 1 – 51);

wherein the data element identifies a notification type for the notification, an originating IP address for the notification and/or a destination IP address for the notification (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55) and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55).

9. Regarding claim 82, Khanolkar in view of Wiley further show a system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising at least one processor programmed to implement:

means for capturing, in a first data structure of a plurality of data structures (Wiley, col. 4 lines 40 – 65), a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event (Khanolkar, col. 2 lines 10 – 67, col. 3 lines 57—65, col. 4 lines 15 – 30), the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic (Wiley, col. 6 lines 11 - 35, col. 7 lines 1 – 51);

means for identifying a data element within the notification (Khanolkar, col. 6 lines 2 – 8, col. 7 lines 1 - 3);

means for updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded (Wiley, col. 5 lines 25 – 67, col. 7 lines 1 – 51);

wherein the data element identifies a notification type for the notification, an originating IP address for the notification and/or a destination IP address for the notification (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55) and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred (Khanolkar, col. 6 lines 1 – 24, col. 4 lines 11 – 55).

10. Regarding claims 10, 23, 36 and 91, Khanolkar in view of Wiley further show wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet (Khanolkar, col. 2 line 40 and col. 5 lines 10 – 50).

11. Regarding claims 11, 24, 37 and 92, Khanolkar in view of Wiley further show accessing the index to determine, based on the indication, the location of the data element within the first data structure, and accessing the data element at the location (Wiley, col. 4 lines 31 - 67, col. 7 lines 1 - 51).

12. Regarding claims 12, 25, 38 and 93, Khanolkar in view of Wiley further show creating a summery based at least in part on a presence of the data element within the notification (Wiley, col. 4 lines 31 - 67, col. 7 lines 1 - 51).

13. Regarding claims 13, 26, 39 and 94, Khanolkar in view of Wiley further show an act comprising accessing the summary to determine the presence of the data element within the first data structure (Wiley, col. 4 lines 31 - 67, col. 7 lines 1 - 51).

14. Regarding claims 109, 114, 119 and 124, Khanolkar in view of Wiley further show wherein the data element identifies a notification type for the notification (Khanolkar, col.6 lines 59 – 65, col. 7 lines 23 - 59).

15. Regarding claims 110, 115, 120 and 125, Khanolkar in view of Wiley further show wherein the data element identifies a originating IP address for the notification (Khanolkar, col. 6 lines 3 – 14 and Wiley col. 4 lines 4 – 8, col. 4 lines 51 -57).

16. Regarding claims 111, 116, 121 and 126, Khanolkar in view of Wiley further show wherein the data element identifies a destination IP address for the notification (Wiley col. 4 lines 4 – 8, col. 4 lines 51 -57).

17. Regarding claims 112, 117, 122 and 127, Khanolkar in view of Wiley further show wherein the characteristic comprises an IP address of the node (Khanolkar, col. 6 lines 3 – 14 and Wiley col. 4 lines 4 – 8, col. 4 lines 51 -57).

18. Regarding claims 113, 118, 123 and 128, Khanolkar in view of Wiley further show wherein the characteristic comprises a time period during which the notification occurred (Khanolkar, col. 6 lines 3 - 14).

19. Claims 2, 3, 15, 16, 28, 29, 83, and 84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar in view of Wiley as applied to claims 1, 14, 27 and 82 above, further in view of Martenson (US 6,219,708 B1).

20. Regarding claims 2, 15, 28 and 83, Khanolkar in view of Wiley show claims 1, 14, 27 and 82.

Khanolkar in view of Wiley do not explicitly show storing the first data structure in a non-volatile storage.

Martenson shows storing the data structure in a non-volatile storage (col. 6 lines 43 – 55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of in view of Wiley with that of Martenson in order to ensure that the data formulated, filtered and processed by the method of Khanolkar is archived for future use on a common and well-understood storage mechanism.

21. Regarding claims 3, 16, 29 and 84, Khanolkar in view of Wiley and Martenson further show storing the first data structure in a file system in the non-volatile storage (Martenson, col. 6 lines 43 - 55).

22. Claims 4, 17, 30 and 85 rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar in view of Wiley and Martenson and as applied to claims 3, 16, 29 and 84 above, and further in view of Richard et al. (US 2005/0015461 A1), hereafter Richard.

Khanolkar in view of Wiley and Martenson show claims 3, 16, 29 and 84.

Khanolkar in view of Wiley Martenson do not explicitly show the file system is a hierarchical file system.

Richard shows where the file system is a hierarchical file system ([111]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Khanolkar in view of Wiley and Martenson with that of Richard in order to utilize a common type of file system (Richard, [111]).

23. Claims 7, 20, 33 and 88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar in view of Wiley, further in view of Microsoft Computer Dictionary, 5th Edition.

24. Regarding claims 7, 20, 33 and 88, Khanolkar in view of Wiley show claims 1, 14, 27 and 82.

Khanolkar in view of Wiley do not explicitly show where the data structure is a file.

Microsoft Computer Dictionary shows files (pgs. 2 - 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Khanolkar in view of Wiley with that of Microsoft Computer Dictionary in order to utilize common ideas in computing environments.

25. Claims 8, 9, 21, 22, 34, 35, 89 and 90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar in view of Wiley and Martenson as applied to claims 2, 15, 28 and 83 above further in view of Microsoft Computer Dictionary, 5th Edition.

26. Regarding claims 8, 21, 34 and 89, Khanolkar in view of Wiley and Martenson show claims 2, 15, 28 and 83.

Khanolkar in view of Wiley and Martenson do not explicitly show an act of compressing the data structure.

Microsoft Computer Dictionary shows compression of files, such as data structures (pgs. 2-3 and 4 -5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Khanolkar in view of Wiley and Martenson with that

of Microsoft Computer Dictionary in order to utilize common ideas in computing environments, as well as to optimize the storage size of the data structure.

Khanolkar in view of Wiley, Martenson and Microsoft Computer Dictionary thus show claims 8, 21, 34 and 89.

27. Regarding claims 9, 22, 35 and 90, Khanolkar in view of Wiley, Martenson and Microsoft Computer Dictionary further show act of creating a digital signature for the data structure (Microsoft Computer Dictionary, pgs. 2 – 3 and 6).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIlwinen whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2442

John MacIlwinen

(571) 213 - 6095